



アプリケーション連携ソリューション

AMF-SECurity

標的型サイバー攻撃拡散防止対策

AT-AR4050Sシリーズ × AMF-SEC

5年保証



AT-AR4050S-5G-Z1



サイバー攻撃感染端末を エッジスイッチで遮断隔離！拡散防止！

■SDNによる新たなソリューション

アライドテレシスのSDN/アプリケーション連携ソリューション「AMF-SEC (旧名Secure Enterprise SDN)」と、次世代ファイアウォール&VPNルーター「AT-AR4050S/AT-AR4050S-5G」との連携により、サイバー攻撃・脅威感染の可能性がある被疑端末の通信遮断および検疫隔離を動的に行う情報漏洩被害拡散防止対策ソリューションです。
仮にマルウェアが被疑端末上でIPアドレスを変更し、通信継続を試みても、MACアドレス制御によりアクセス管理および制御を行うため確実に被疑端末を遮断隔離することが可能です。

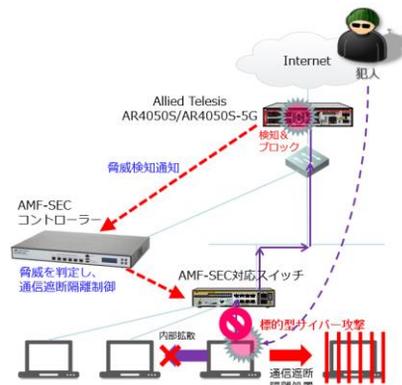
◆ 標的型サイバー攻撃対策

AT-AR4050S/AT-4050S-5G は、次世代ファイアウォール搭載のUTM&VPNルーターです。IPsecやL2TPv3などのVPN対応や、次世代ファイアウォールで必要不可欠なセキュリティエンジンを搭載し、外部からの攻撃や社内からの情報漏洩を防ぎ、安全なインターネット接続環境を構築できます。

本連携に於いては、脅威検知セキュリティエンジンの内、下記連携対象機能により検出したサイバー攻撃感染端末の通信をエッジスイッチ/無線APにて遮断・隔離し被害の拡散防止を図ります。

- ・IPレピュテーション
- ・ファイアウォール

※ 本図解では混乱を避けるため、コントローラーとして機能させる AMF Security miniライセンス・AMF Plusマスターライセンスを導入しない構成としております。



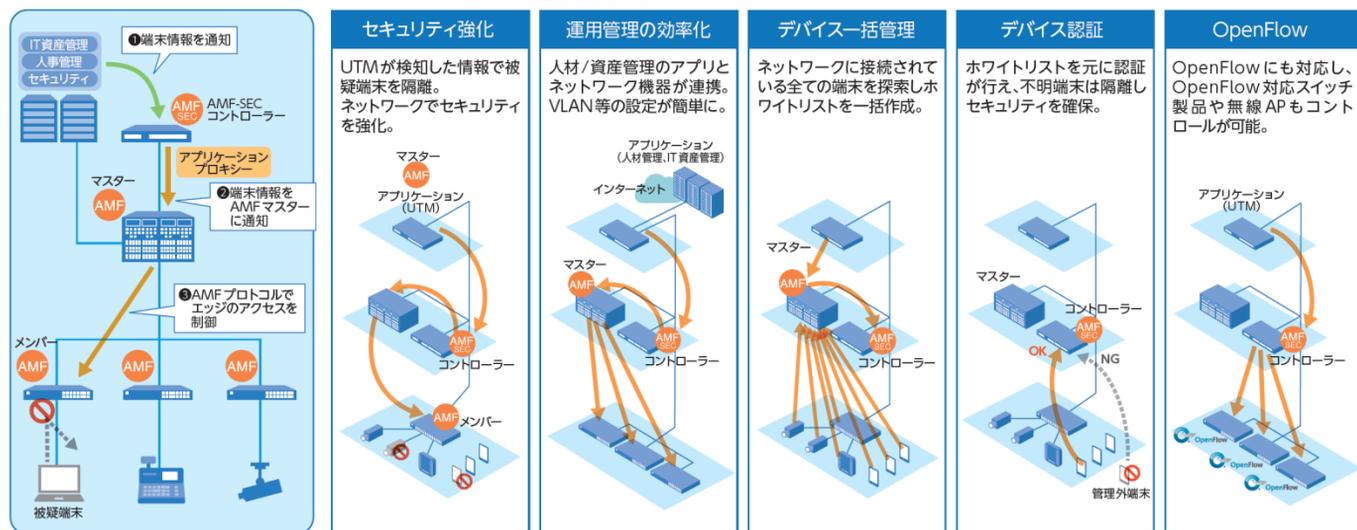
エンタープライズ市場に最適なセキュリティソリューション

「AMF-SECURITY」

～アプリケーション連携による企業向けのSDNを実現～

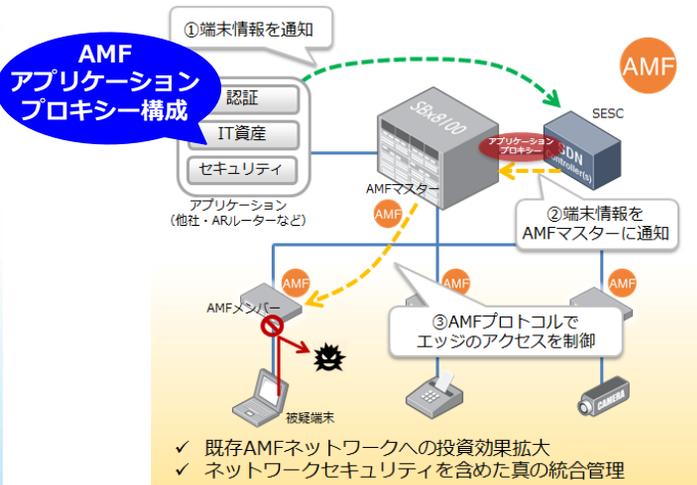
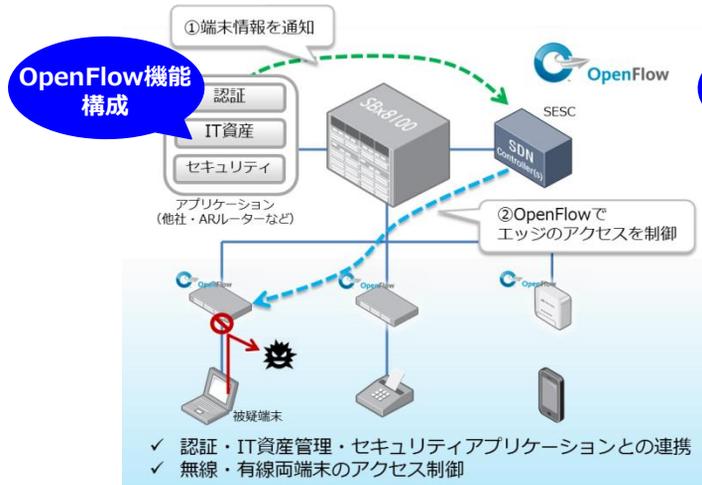
企業のネットワーク運用を最適化するソリューションとしてAMF-SECを開発しました。アプリケーションと連携・連動するネットワークによってユーザートラフィックの動的制御機能をご提供します。セキュリティの強化と、ネットワークの運用にかかるコストの削減、運用負荷の低減を実現しました。以下に、アライドテレシスが提案する「AMF-SEC」およびネットワーク統合管理機能AMFとの連携機能「AMFアプリケーションプロキシ」をご紹介します。

1. 「AMF-SEC」と「AMF」との連携動作



2. OpenFlow構成とAMFアプリケーションプロキシ構成

ネットワーク統合管理機能AMFマスターを介し、各種アプリケーションからの情報により、AMFマスターがエッジのAMFメンバーを制御、端末の通信制御（ホワイトリスト/ブラックリスト制御）を実現します。 ※ 無線AP(AMF-SEC対応AT-TQシリーズ)接続端末のアクセス制御にも対応しております。



本資料に関する
ご質問やご相談は

TEL: 0120-860442
アライドテレシス株式会社

製品の詳しい情報は
(特徴、仕様、マニュアル等)

ホームページ
<http://www.allied-teleasis.co.jp>